Core Vulnerabilities Assessment Management Program (CVAMP) Training

MAJ(P) Mike Anderson, USA
J3 DDAT/HD

CVAMP Background

- Developed by EUCOM, in use since 1998
- Adopted by Air Force in 2002, Navy/Marines in 2003
- Army, other Combatant Commands and DOD agencies/activities do not have an adequate AT/FP vulnerability and requirements management capability
- DoD Directive 2000.12 (AUG 03) directs the JS to maintain a centralized vulnerability database
- Services/Combatant Commands/JS AOs agreed to "Core-VAMP" concept JAN 03 and MOA signed in APR 03
- Joint Staff establishes MOA with Defense Technical Information Center to develop CVAMP in FEB 03

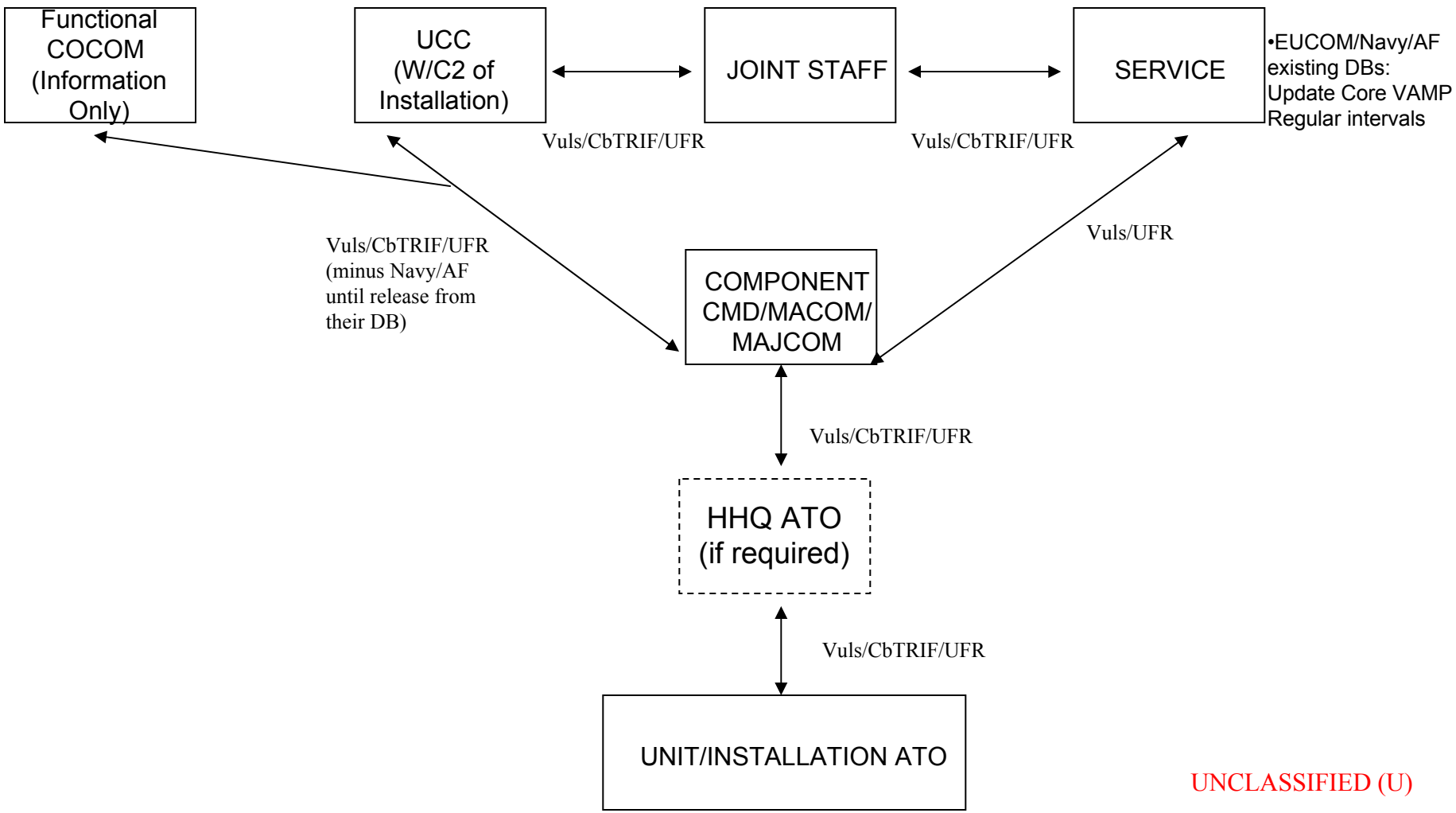
CVAMP Capabilities

- Accessed via the Antiterrorism Enterprise Portal (ATEP) on the SIPRNET
- Tracks and manages AT vulnerabilities per DoDI 2000.16
- Generates justification for requirements to resolve vulnerabilities
- Standardizes and automates AT resource request process; CbT RIF and UFR submissions IAW DepSecDef approved funding prioritization
- Highlights AT readiness shortfalls due to unmitigated vulnerabilities

CVAMP Control of Information

- CVAMP users shall be able to enter and release vulnerabilities through the chain of command to J3.
- CVAMP users shall be able to enter funding requests associated with a vulnerabilities and send the funding requests through the chain of command to J3. Each level of the chain of command shall be able to rank subordinate's funding requests.
- Only authorized users may view/edit the vulnerabilities and funding requests.

CVAMP Data Release Flow



CVAMP Policy/Directives

- Unified Combatant Commands set policy on use of CVAMP
  - Required data input
  - Timelines for data release to HHQ

- Service policy/guidelines do not override Unified Combatant Command

Management Boards

- Identifies and prioritizes system and software requirements
- CVAMP Requirements Management Board (VRMB) is chartered via the CVAMP MOA
  - JS, J3, DDAT/FP
  - DTIC
  - Services
  - Combatant Commanders
  - DoD Agencies and Activities
- VRMB meets twice annually
  - JUL 03
  - MAR 04

Training Objectives

Given access to CVAMP you will be able to:

1. Assign roles in CVAMP
2. Create an organization
3. Create a vulnerability assessment
4. Create an observation
5. Approve and release observations/vulnerabilities
6. Conduct database searches
7. Create a funding request (CbtRIF and UFR)
8. Prioritize and release funding requests